Lebeau Mathéo

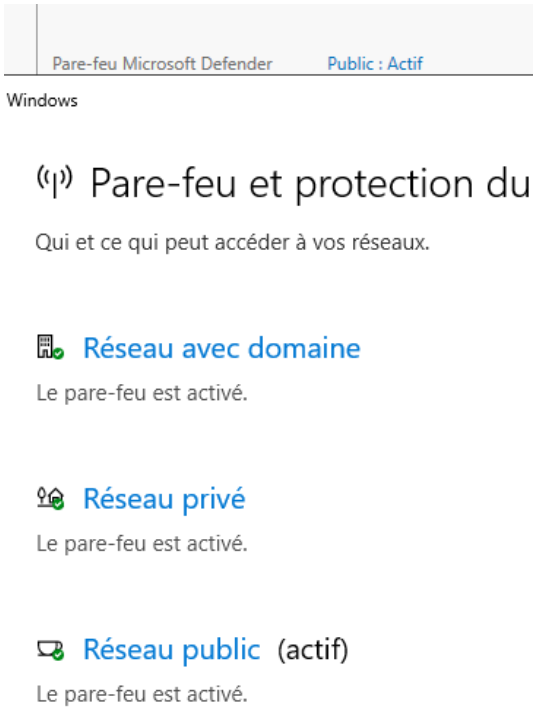
TP Durcissement sécurité AD et serveur + Laps

BTS SIO2

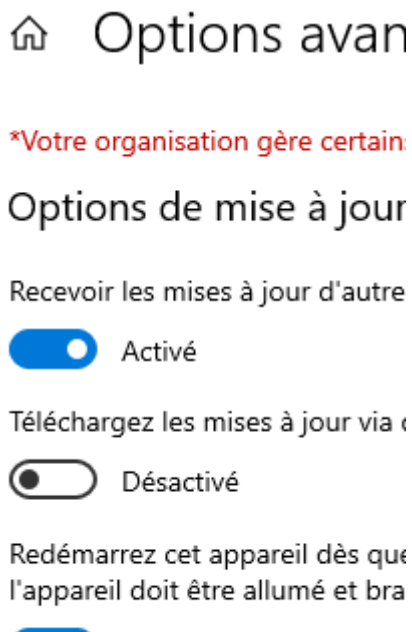
Intro :

Dans ce tp nous allons améliorer la sécurité de notre serveur AD ainsi que notre windows serveur et on finira avec l'installation de windows Laps. Ces mesures visent à améliorer la sécurité pour se défendre de potentielles attaques malveillantes.

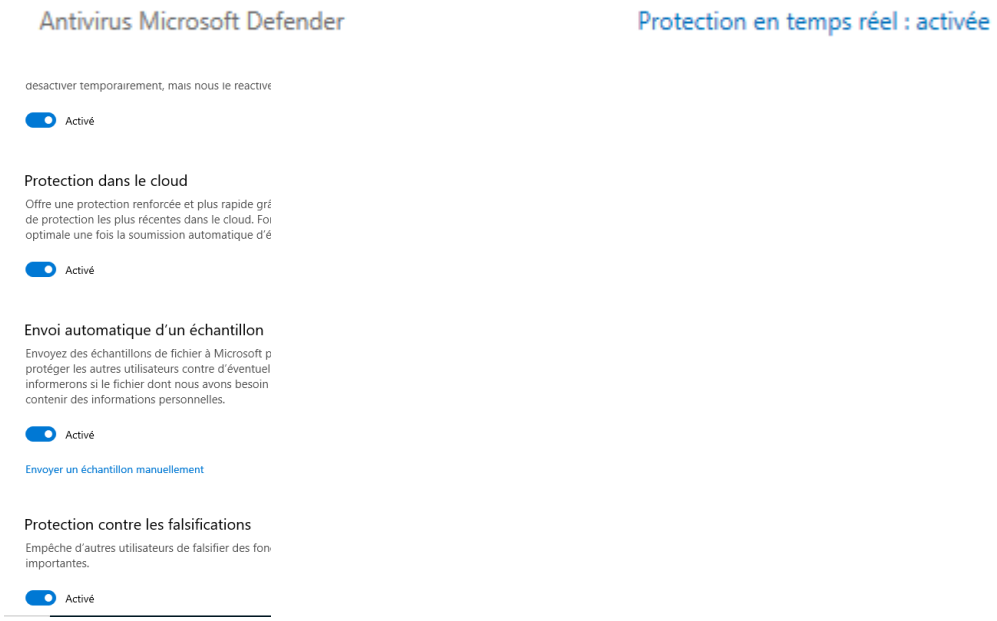
Commençons avec le Durcissement et Sécurité Windows Server.
Rendons-nous sur l'ad et on va réactiver tous les pare-feu désactivés



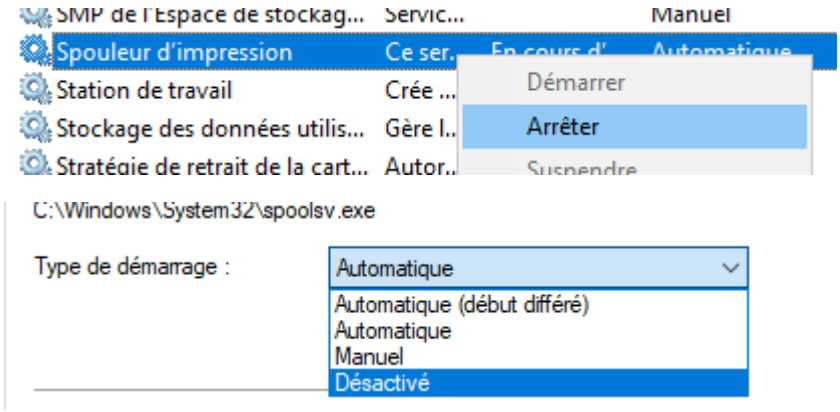
Puis il faut effectuer les mises à jour et cocher les cases suivantes



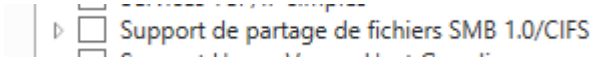
Et dans les paramètres de l'antivirus directement cocher toutes les cases de protection.



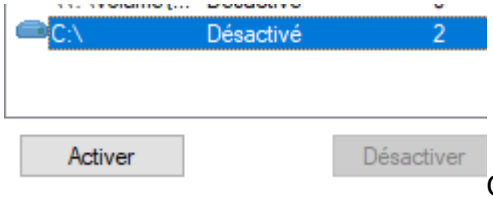
Ensuite comme notre serveur n'utilise pas d'imprimante on va désactiver et arrêter le spouleur d'impression dans les services.



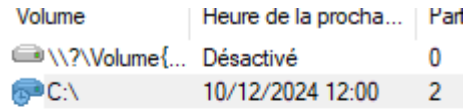
Il faut vérifier aussi à bien désactiver la fonctionnalité smb 1.0 obsolète.



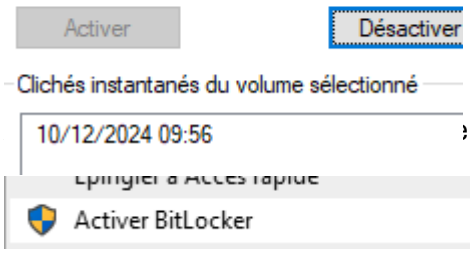
On va ensuite par sécurité activer les clichés instantanés sur notre disque C.



On peut également les planifier si besoin par jours ect.



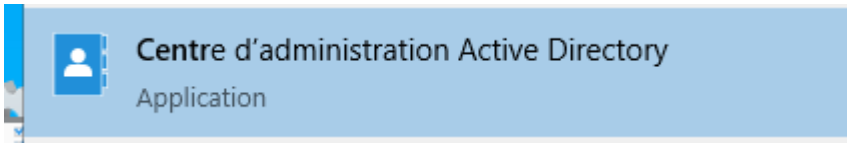
ement avec BitLocker dans les fonctionnalités.



r BitLocker sur le disque

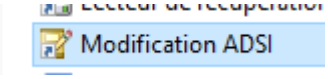
Puis il faudra simplement choisir le répertoire où l'on enregistrera le fichier correspondant à la clé de récupération et enfin il faudra choisir le dernier type de chiffrement.

Deuxième partie pour notre tp on va passer à la Sécurité contrôleur de domaine Active Directory.
On va se rendre dans le centre d'administration.

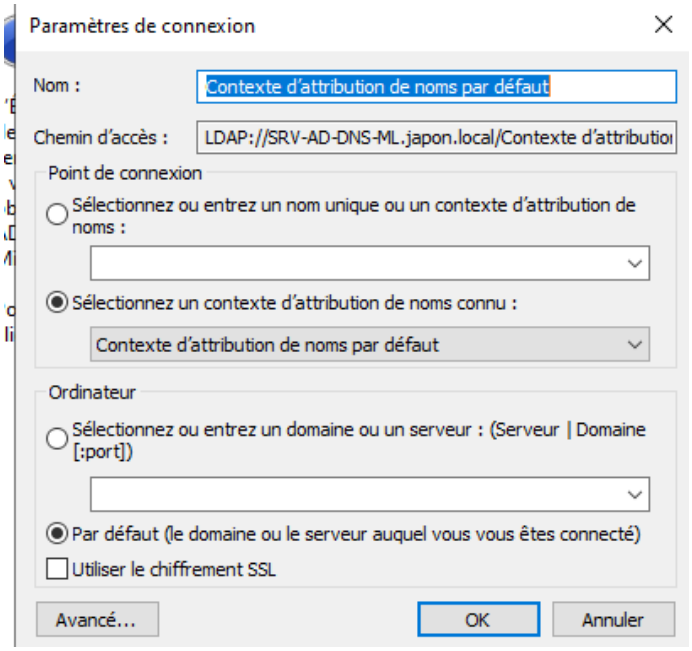


Et on active la corbeille ce qui nous permettra de rétablir les éventuelles suppressions accidentelles.

Ensuite on se rend dans l'outil d'administration suivant.

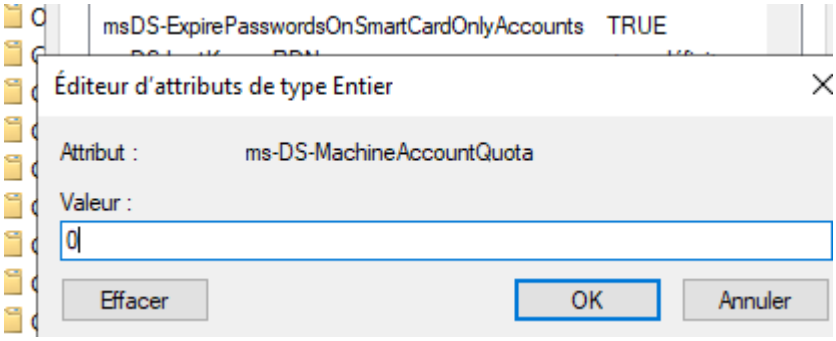


Puis sur action on fait connexion et la fenêtre suivante apparaît.



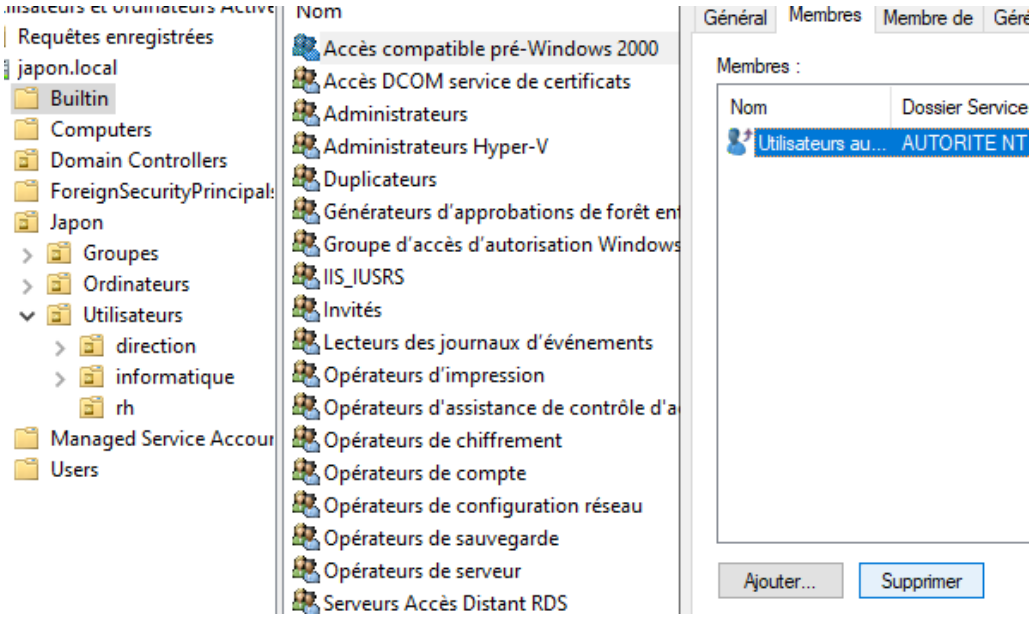
Et on fera juste OK sans rien toucher.

Puis dans les propriétés du domaine dans l'éditeur d'attribut on va chercher



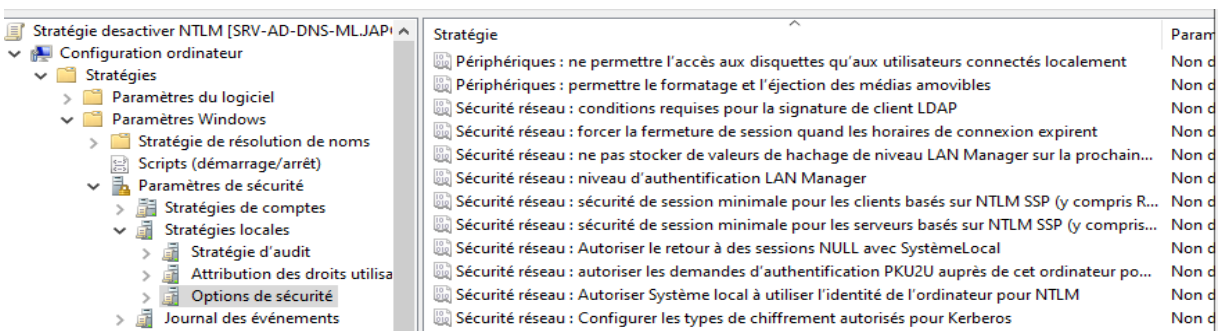
Et en double cliquant dessus on le mettra à 0. Ce paramètre à 0 fera qu'uniquement les admins pourront mettre des machines au domaine.

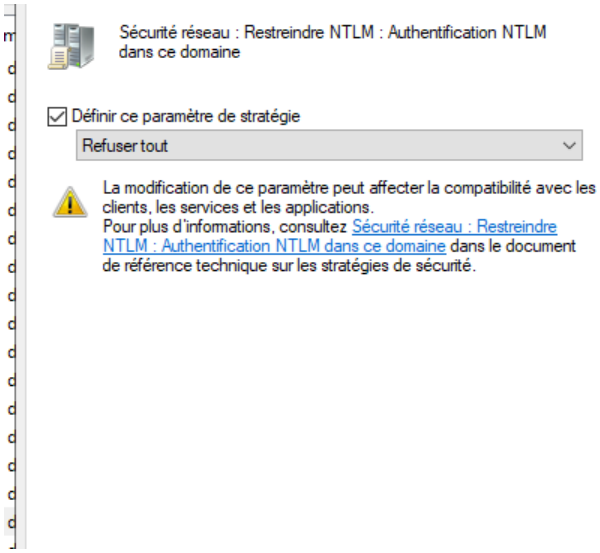
On va maintenant se rendre dans l'ad et supprimer les droits de rétrocompatibilité avant windows 2000



Ensuite dans le gestionnaire de stratégie de groupe.

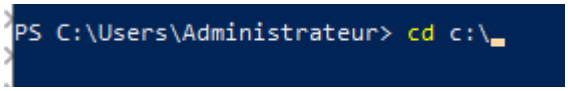
On va Désactiver NTLMv1 et NTLMv2 qui sont des protocoles parfois utilisés mais dangereux.

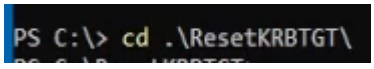


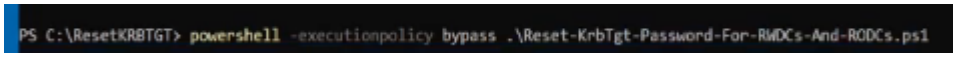


Puis retournons sur l'ad et on va faire quelque manipulation pour veiller a la bonne sécurité de l'utilisateur kerberos qui sert a l'authentification.

Et on va lancer le powershell et faire quelques commandes.



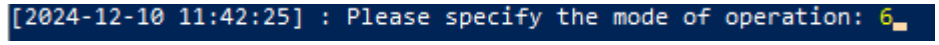




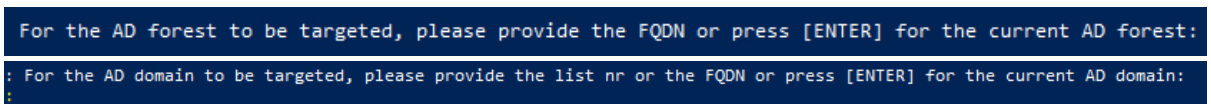
powershell -executionpolicy bypass .\Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1

Ensuite une nouvelle fenêtre s'ouvre.

Puis quelques étapes à suivre.

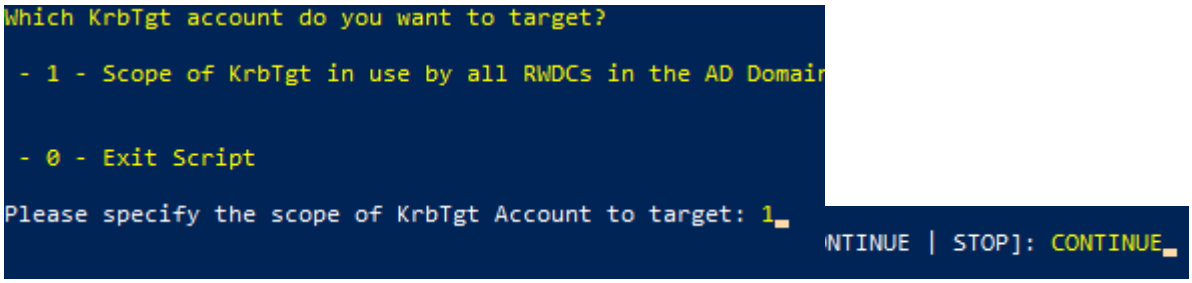


Juste entrée pour celui en dessous



De même.

Puis



| pwdLastSet 10/12/2024 11:47:33 Paris, Madrid Le mot de passe à bien été changé on a maintenant terminé la sécurisation de l'ad et on va passer a la dernière partie avec l'installation de windows laps